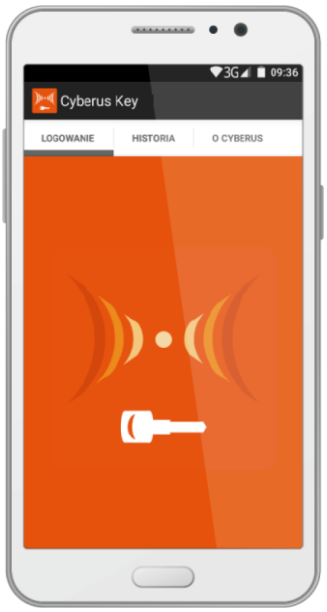
CYBERUSLABS

BEZPIECZNY ŚWIAT



CYBERUS KEY

Rozwiązanie dla Dyrektywy PSD2 (Dyrektywa (EU) 2015/2366)

Wymagania dla banków & operatorów zewnętrznych (TPP - Third Part Providers)

CYBERUS KEY – rozwiązanie dla wymagań stawianych przez dyrektywę PSD2 dla banków oraz TPPs.

Dyrektywa PSD2 umożliwia klientom banków, zarówno indywidualnym jak i biznesowym, korzystanie z usług operatorów zewnętrznych do dokonywania transakcji bankowych. Klienci będą mieli możliwość wyboru operatora usług np. Google do płacenia rachunków oraz przelewów P2P (person-to-person). Operatorzy zewnętrzni (TPP) będą mogli przeprowadzić transakcje, które do tej pory były zarezerwowane dla banków i w związku z tym będą również mieli możliwość dostępu do danych klientów banków. Banki będą miały natomiast obowiązek zapewnienia operatorom zewnętrznym (TPP) dostępu do kont bankowych klientów poprzez otwarte API. Umożliwi to operatorom zewnętrznym (TPP) oferowanie usług finansowych w oparciu o dane i infrastrukturę pochodzącą z banku.

Celem dyrektywy jest poprawa obecnych przepisów UE dotyczących płatności elektronicznych. Dyrektywa UE ustanawia również przepisy dotyczące między innymi: rygorystycznych wymogów bezpieczeństwa płatności elektronicznych i ochrony danych finansowych konsumentów, które gwarantują bezpieczne uwierzytelnienie i zmniejszają ryzyko oszustw finansowych;

Dyrektywa weszła w życie w dniu 12 stycznia 2016 roku. Państwa członkowskie UE mają czas do dnia 13 stycznia 2018 r. na jej pełną implementację.

Wpływ dyrektywy PSD2.

Nowa dyrektywa wprowadza zasadnicze zmiany, które obejmują:

1) inicjowanie płatności przez firmy zewnętrzne: dostawcy inicjujący usługi płatnicze (PISP) będą w stanie dokonać płatności online z rachunku bankowego płatnika,

2) ochrona płatności online i dostępu do konta poprzez wprowadzenie nowych wymogów bezpieczeństwa dotyczących płatności elektronicznych oraz dostępu do konta.

Banki będą musiały udostępnić swoją infrastrukturę zewnętrznym usługodawcom oferując interfejs API. Będą zmuszone do przyznania im dostępu do płatności internetowych swoich klientów w regulowany i bezpieczny sposób.

Dyrektywa PSD2 nakazuje operatorom zewnętrznym (TPP) pytać klientów o zgodę na wykorzystanie ich danych bankowych. W przypadku odpowiedzi pozytywnej operator-sprzedawca otrzyma zapłatę bezpośrednio z banku, bez pośredników.

Bezpośrednie połączenie między sprzedawcami a bankami zostanie uzyskane dzięki API.

Wymagania dotyczące silnego uwierzytelnienia klienta

Dyrektywa PSD2 daje możliwość dostępu operatorom zewnętrznym do kont (XS2A), poprzez korzystanie z interfejsu API. Dodatkowo zapewnia połączenie bezpośrednie między operatorem i bankiem oraz zdolność do konsolidacji informacji w jednej platformie.

Jednocześnie operator zewnętrzny (TPP), aby obsługiwać płatności online musi zapewnić, że posiada i oferuje użytkownikom najwyższy poziom zabezpieczeń również po swojej stronie.

Silny system uwierzytelnienia klienta – Cyberus Key

Cyberus Key oferuje możliwość stworzenia pomostu łączącego banki i operatorów zewnętrznych (TPP). Jest to jedna z głównych cech wyróżniających **Cyberus Key** spośród wszystkich obecnie oferowanych systemów.

Ideą systemu **Cyberus Key** jest:

- dokonywanie w pełni bezpiecznego logowania do konta użytkownika bez konieczności używania hasła czy jakichkolwiek danych pozwalających na identyfikację użytkownika,

- przeprowadzenie w pełni bezpiecznych transakcji bez wymiany danych dotyczących użytkownika,

- zabezpieczenie anonimowego trybu online, podczas gdy operator posiada pełną informację o odbiorcy,

- generowanie informacji o logowaniu i transakcjach takich jak czas, data czy geolokalizacja.

Cyberus Key to platforma identyfikacji, który jest odpowiedzią na wymogi dyrektywy PSD2 stawiane bankom i operatorom zewnętrznym (TPP). System umożliwia klientom banku łatwy, szybki i w pełni bezpieczny dostęp do konta oraz ochronę w trakcie dokonywania wszelkich transakcji online.

Istotnym elementem systemu **Cyberus Key** jest Cyberus Key Authentication Server (CAS). Instalacja systemu **Cyberus Key** wraz z CAS w ramach infrastruktury IT banku zapewnia bezpieczeństwo danych użytkowników, za które bank jest odpowiedzialny. Cyberus Key oferuje jednak znacznie więcej.

Dla każdego zarejestrowanego w systemie **Cyberus Key** klienta banku tworzony jest anonimowy profil na Cyberus Key Authentication Server (CAS), zainstalowanym w ramach infrastruktury informatycznej banku. Anonimowy profil użytkownika i dane związane z logowaniem są jedynymi przechowywanymi danymi na tym serwerze. I tylko te anonimowe dane używane są do potwierdzenia logowania i dokonywania transakcji. Oznacza to, że żadne informacje mogące pozwolić na zidentyfikowanie użytkownika nie są wykorzystywane do logowania lub potwierdzania płatności. Połączenie anonimowego profilu użytkownika i ID dokonywanych transakcji z danymi osobowymi użytkownika dokonuje się tylko i wyłącznie miedzy CAS a bazą danych klientów banku w ramach wewnętrznej infrastruktury informatycznej banku. W związku z tym, żadne dane użytkownika, jak hasła, dane, osobowe, etc nie są przekazywane na zewnątrz nie są one narażone na kradzież przez cyberprzestępców.

Jedyne elementy, który wykorzystuje **Cyberus Key** w procesie autoryzacji to:

- jednorazowy kod, który wykorzystuje metodologię One-Time-Pad i jest generowany przez HSM (Hardware Security Module),

-unikatowy identyfikator i dane profilu związane z aplikacją oraz urządzeniem mobilnym użytkownika.

Pozwala to zabezpieczyć wszelkie dane osobowe użytkownika w ramach wewnętrznej infrastruktury informatycznej banku bez przekazywania tych informacji operatorom zewnętrznym (TPP) podczas procesu logowania, dokonywania płatności czy innych operacji. Jednocześnie dzięki systemowi **Cyberus Key** bank oraz TPP są w stanie wykonywać transakcje online bez ryzyka przechwycenia danych użytkownika przez nieautoryzowaną stronę. W ten sposób eliminowane są nadużycia związane z kradzieżą danych uwierzytelniających.

Dlaczego jest to tak ważne w przypadku dyrektywy PSD2? Jedną z największych obaw banków związanych z dyrektywą PSD2 jest udostępnianie danych swoich klientów operatorom zewnętrznym (TPP). Kolejnym wyzwaniem jest stworzenie wspólnej platformy, która będzie używać interfejsu (API) do połączenia z operatorami zewnętrznymi.

Cyberus Key jest odpowiedzią na wszystkie te wyzwania. **Cyberus Key** to istniejąca już platforma z gotowym API, która oferuje możliwość anonimowego połączenia typu Single-Sign-On pomiędzy bankiem a TPP. W przeciwieństwie do obecnych rozwiązań SSO, które przekazują dane uwierzytelniające użytkownika, proces logowania z wykorzystaniem **Cyberus Key** jest anonimowy. Używany jest jedynie jednorazowy kod i anonimowy profil klienta dla tej operacji. Dane użytkownika nie są przekazywane podczas dokonywania operacji.

Jak rozwiązać problem wymagań związanych z PSD2? Każdy zewnętrzny operator, który chce dokonywać transakcji dla klientów banków musi być zintegrowany z API banku. System **Cyberus Key** daje gotowe rozwiązanie dla banków i TPP. Oferuje możliwość współpracy i wykonywania transakcji online bez udostępniania poświadczeń klientów ani żadnych danych operatorom zewnętrznym w trakcie tego procesu. W przypadku implementacji **Cyberus Key** w banku wystarczy, że klienci banku są również użytkownikami systemu **Cyberus Key** zainstalowanego przez operatora zewnętrznego (TPP). Jest też możliwy wariant odwrotny kiedy to zewnętrzny usługodawca, który wdroży **Cyberus Key** będzie mieć własną bazę danych klientów, którzy będąc jednocześnie klientami banku są w ten sposób chronieni również przez wewnętrzne zabezpieczenia infrastruktury informatycznej banku.

W tym przypadku, przy dokonywaniu transakcji przez klienta w jego banku nie istnieją informacje lub dane osobowe przekazywane między bankiem a TPP. Podczas przeprowadzania transakcji przez operatora zewnętrznego na rzecz klienta banku, w tym samym czasie wszystkie trzy strony (klient, bank i TPP) otrzymają informacje na temat transakcji, ale jej dane przekazywane między stronami nie będą zawierały żadnych danych pozwalających na zidentyfikowanie tożsamości klienta lub danych samej transakcji. Technologia **Cyberus Key** eliminuje w ten sposób największe zagrożenie związane z przekazywaniem danych użytkownika oraz danych transakcji podczas dokonywania jej online jakimi są kradzież danych użytkownika i zmiana danych transakcji.

Źródła:

http://ec.europa.eu/finance/payments/framework/index_en.htm

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

http://fintechnews.ch/moneytransfer/eus-payment-services-directive-psd2-what-it-is-and-why-it-matters/6959/

https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/